

information on services for individuals with disabilities, or to request special assistance during the meeting, please contact Sandra L. Taylor, Designated Federal Officer, DHS Data Privacy and Integrity Advisory Committee, as soon as possible.

To facilitate public participation, we invite public comment on the issues to be considered by the Committee as listed in the **SUPPLEMENTARY INFORMATION** section below. A public comment period will be held during the meeting, and speakers are requested to limit their comments to 3 minutes. If you would like to address the Committee at the meeting, we request that you register in advance by contacting Sandra L. Taylor at the address provided below. The names and affiliations of individuals who address the Committee will be included in the public record of the meeting. Please note that the public comment period may end before the time indicated, following the last call for comments. Advanced written comments or comments for the record, including persons who wish to submit comments and who are unable to participate or speak at the meeting, should be sent to Sandra L. Taylor, Designated Federal Officer, DHS Data Privacy and Integrity Advisory Committee, by January 24, 2023. All submissions must include the Docket Number (DHS-2023-0001) and may be submitted by any one of the following methods:

- *Federal eRulemaking Portal*: <http://www.regulations.gov>. Follow the instructions for submitting comments.

- *E-mail*: [PrivacyCommittee@hq.dhs.gov](mailto:PrivacyCommittee@hq.dhs.gov). Include the Docket Number (DHS-2023-0001) in the subject line of the message.

- *Mail*: Sandra L. Taylor, Designated Federal Officer, Data Privacy and Integrity Advisory Committee, Department of Homeland Security, 2707 Martin Luther King, Jr. Avenue SE, Mail Stop 0655, Washington, DC 20598.

*Instructions*: All submissions must include the words "Department of Homeland Security Data Privacy and Integrity Advisory Committee" and the Docket Number (DHS-2023-0001). Comments received will be posted without alteration at <http://www.regulations.gov>, including any personal information provided. You may wish to review the Privacy & Security Notice found via a link on the homepage of [www.regulations.gov](http://www.regulations.gov).

The DHS Privacy Office encourages you to register for the meeting in advance by contacting Sandra L. Taylor, Designated Federal Officer, DHS Data Privacy and Integrity Advisory Committee, at [PrivacyCommittee@](mailto:PrivacyCommittee@)

[hq.dhs.gov](http://hq.dhs.gov). Advance registration is voluntary. The Privacy Act Statement below explains how DHS uses the registration information you may provide and how you may access or correct information retained by DHS, if any.

*Docket*: For access to the docket to read background documents or comments received by the DHS Data Privacy and Integrity Advisory Committee, go to <http://www.regulations.gov> and search for docket number DHS-2023-0001.

**FOR FURTHER INFORMATION CONTACT:**

Sandra L. Taylor, Designated Federal Officer, DHS Data Privacy and Integrity Advisory Committee, Department of Homeland Security, 2707 Martin Luther King, Jr. Avenue SE, Mail Stop 0655, Washington, DC 20598, by telephone (202) 343-1717, or by email to [PrivacyCommittee@hq.dhs.gov](mailto:PrivacyCommittee@hq.dhs.gov).

**SUPPLEMENTARY INFORMATION:** Notice of this meeting is given under the Federal Advisory Committee Act (FACA). The DHS Data Privacy and Integrity Advisory Committee provides advice at the request of the Secretary of Homeland Security and the DHS Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues within DHS that relate to personally identifiable information, as well as data integrity, transparency, information sharing, and other privacy-related matters. The Committee was established by the Secretary of Homeland Security under the authority of 6 U.S.C. 451.

**Proposed Agenda**

The Chief Privacy Officer will provide the Committee with an update on Privacy Office activities and discuss the Privacy Office's 2023 priorities. In addition, the Committee will receive an update from the Director of the Department's Center for Accelerating Operational Efficiency on privacy enhancing technologies. If you wish to submit written comments, you may do so in advance of the meeting by submitting them to Docket Number (DHS-2023-0001) at [www.regulations.gov](http://www.regulations.gov) or by forwarding them to the Committee at the locations listed under the **ADDRESSES** section. The final agenda will be posted on or before January 23, 2023, on the Committee's website at [www.dhs.gov/dhs-data-privacy-and-integrity-advisory-committee-meeting-information](http://www.dhs.gov/dhs-data-privacy-and-integrity-advisory-committee-meeting-information).

**Privacy Act Statement: DHS's Use of Your Information**

*Authority*: DHS requests that you voluntarily submit this information

under its following authorities: The Federal Records Act, 44 U.S.C. 3101; the FACA, 5 U.S.C. appendix; and the Privacy Act of 1974, 5 U.S.C. 552a.

*Principal Purposes*: When you register to attend a DHS Data Privacy and Integrity Advisory Committee meeting, DHS collects your name, contact information, and the organization you represent, if any. We use this information to contact you for purposes related to the meeting, such as to confirm your registration, to advise you of any changes to the meeting, or to assure that we have sufficient materials to distribute to all attendees. We may also use the information you provide for public record purposes such as posting publicly available transcripts and meeting minutes.

*Routine Uses and Sharing*: In general, DHS will not use the information you provide for any purpose other than the Principal Purposes and will not share this information within or outside the agency. In certain circumstances, DHS may share this information on a case-by-case basis as required by law or as necessary for a specific purpose, as described in the DHS/ALL-002 Mailing and Other Lists System of Records Notice (November 25, 2008, 73 FR 71659).

*Effects of Not Providing Information*: You may choose not to provide the requested information or to provide only some of the information DHS requests. If you choose not to provide some or all of the requested information, DHS may not be able to contact you for purposes related to the meeting.

*Accessing and Correcting Information*: If you are unable to access or correct the information provided by using the method that you originally used to submit it, you may direct your request in writing to the DHS Deputy Chief FOIA Officer at [foia@hq.dhs.gov](mailto:foia@hq.dhs.gov). Additional instructions are available at <http://www.dhs.gov/foia> and in the DHS/ALL-002 Mailing and Other Lists System of Records referenced above.

**Lynn Parker Dupree,**

*Chief Privacy Officer, Department of Homeland Security.*

[FR Doc. 2023-00699 Filed 1-13-23; 8:45 am]

**BILLING CODE P**

**DEPARTMENT OF HOMELAND SECURITY**

**Transportation Security Administration**

**Exemption for Exclusive Area Agreements at Certain Airports**

**AGENCY:** Transportation Security Administration, DHS.

**ACTION:** Notice.

**SUMMARY:** The Transportation Security Administration (TSA) has statutory authority to grant an exemption from a regulation if TSA determines the exemption is in the public interest. TSA is granting an exemption from an aviation security regulation to permit eligible airport operators to enter into Exclusive Area Agreements (EAA) with Amazon Air, subject to requirements set forth in the Exemption. Also, TSA is rescinding an exemption issued on July 26, 2021, that permitted three airports to enter into EAAs with Amazon Air, as they are now covered by this exemption.

**DATES:** This Exemption becomes effective on January 17, 2023 and remain in effect until modified or rescinded by TSA through a notice published in the **Federal Register**.

**FOR FURTHER INFORMATION CONTACT:** Eric Byczynski, Airport Security Programs, Aviation Division, Policy, Plans, and Engagement; *eric.byczynski@tsa.dhs.gov*.

**SUPPLEMENTARY INFORMATION:****Purpose**

TSA's regulations provide that airport operators may enter into EAAs only with aircraft operators or foreign air carriers that have a security program under 49 CFR part 1544 or 1546, subject to TSA approval of an amendment to each airport operator's airport security program (ASP). *See* 49 CFR 1542.111. Amazon Air is not an aircraft operator or foreign air carrier, but conducts significant operations at airports on behalf of aircraft operators. In July 2021,<sup>1</sup> TSA determined it was in the public interest to grant an exemption to section 1542.111 to three airports to permit them to enter into EAAs with Amazon Air. That exemption applied to Cincinnati/Northern Kentucky International Airport (CVG), Baltimore/Washington International Thurgood Marshall Airport (BWI), and Chicago Rockford International Airport (RFD). TSA determined that the public interest was served because the EAAs would create operational and economic efficiencies for the airport operators and Amazon Air, to the economic benefit of the public and without detriment to security. The exemption permitted the airports to leverage significant private sector technologies with respect to access control and monitoring systems that enhance security and minimize insider threat. The exemption also facilitated the rapid hiring of significant numbers of new personnel to support

Amazon Air's expanded presence at these locations, aiding the economy in the surrounding areas. Finally, under the exemption, TSA exercises direct regulatory oversight of Amazon Air concerning the security functions they perform under the EAAs.

As discussed below, TSA has determined that the Exemption should be issued for all airport operators that have an ASP as set forth in 49 CFR 1542.103(a)–(b), subject to TSA approval and the ability of the airport operators and Amazon Air to satisfy the requirements set forth in this Exemption.<sup>2</sup> Furthermore, this Notice rescinds the previous Exemption TSA published in 2021.

**Background***Airport Security*

TSA administers a comprehensive regulatory program to govern the security of aviation, including standards for domestic airport operators, domestic aircraft operators, and foreign air carriers. The security requirements for domestic airport operators are codified at 49 CFR part 1542 and include minimum standards for access control procedures, identification (ID) media, criminal history record checks (CHRCs) of airport workers, law enforcement support, training, contingency plans, TSA inspection authority, and incident management. These regulations require airport operators to conduct specified security measures in the secured area,<sup>3</sup> air operations area (AOA), and security identification display area (SIDA) of the airport. Part 1542 requires airports to develop and follow TSA-approved ASPs<sup>4</sup> that establish security procedures specific to each airport, and Security Directives, which apply to all airports.

TSA recognizes that, in certain circumstances, these security measures may be performed more effectively or efficiently by another TSA-regulated party such as an aircraft operator or foreign air carrier, operating on the airport. Therefore, under 49 CFR 1542.111, TSA may approve an amendment to an airport's ASP that permits the airport operator to execute a legally binding EAA with an aircraft operator<sup>5</sup> or foreign air carrier.<sup>6</sup> Under the EAA, the aircraft operator or foreign air carrier assumes responsibility from

the airport operator for specified ASP security measures in all or specified portions of the secured area, AOA, or SIDA.<sup>7</sup> TSA requires the EAA to be in writing, and signed by the airport operator and the aircraft operator or foreign air carrier.<sup>8</sup> TSA also prescribes in detail the required contents of the EAA, including a description of the measures that become the responsibility of the aircraft operator or foreign air carrier.<sup>9</sup>

EAAs are an established part of TSA's regulatory structure for airport operators, and have been commonly used since 1978.<sup>10</sup> Currently, there are more than 70 EAAs in place between aircraft operators or foreign air carriers and domestic airport operators. A typical example for the use of an EAA is where an entire airport terminal is serviced exclusively by one aircraft operator. At these locations, TSA conducts standard compliance inspections, and may issue violations of the security standard set forth in the EAA against the aircraft operator or foreign air carrier that holds the EAA.

An "authorized representative" is a person who performs TSA-required security measures as an agent of a TSA-regulated party. Although the authorized representative may perform the measures, the TSA-regulated party remains responsible for completion, and TSA holds the TSA-regulated party primarily accountable through enforcement action of any violations. TSA may also hold the authorized representative accountable if it causes the regulated party's violation.<sup>11</sup>

*Entities Subject to the Exemption*

This Exemption applies to airport operators with a complete or supporting ASP as set forth in 49 CFR 1542.103(a) and (b), and Amazon Air. Amazon Air is a subsidiary of *Amazon.com, Inc.*, an American multinational technology company based in Seattle, Washington engaged in e-commerce, cloud computing, digital streaming, artificial intelligence, and cargo shipping. Amazon reports that less than 20 percent of Amazon's cargo is shipped by air. Due in part, however, to the COVID-19 public health crisis and impact on the economy, cargo shipment has increased dramatically, with a corresponding relative increase in the total volume of air cargo. The increases are due, in part, to the COVID pandemic, the public's heightened

<sup>2</sup> Note that TSA will consider permitting other entities that are similarly situated to Amazon Air to enter into EAAs with airport operators.

<sup>3</sup> *See* 49 CFR 1540.5 for definitions of terms used throughout this exemption.

<sup>4</sup> *See* 49 CFR 1542.105(a).

<sup>5</sup> *See* 49 CFR part 1544.

<sup>6</sup> *See* 49 CFR part 1546.

<sup>7</sup> 49 CFR 1542.111(a).

<sup>8</sup> 49 CFR 1542.111(b).

<sup>9</sup> *Id.*

<sup>10</sup> *See* 43 FR 60792 (Dec. 28, 1978).

<sup>11</sup> *See* 49 CFR 1540.105.

<sup>1</sup> *See* 86 FR 40072, Exemption for Exclusive Area Agreements at Certain Airports (July 26, 2021).

reliance on online shopping for basic goods, and the Nation's need to move supplies quickly. Amazon Air estimates that these trends will not significantly diminish when the COVID pandemic subsides.

Amazon Air maintains operations at various domestic and international airports. Amazon Air owns air cargo aircraft, but does not operate the aircraft itself and is not an aircraft operator for purposes of TSA's regulations. Amazon Air leases the aircraft to certain aircraft operators holding TSA full all-cargo security programs.<sup>12</sup> Amazon Air then acts as an authorized representative for these full all-cargo aircraft operators<sup>13</sup> at certain airports.

As an authorized representative, Amazon Air performs security functions under TSA's Full All-Cargo Aircraft Operator Standard Security Program on behalf of the aircraft operators, including the responsibility for preventing access to both aircraft and the cargo bound for those aircraft, and providing the Ground Security Coordinator, the individual at the facility responsible for coordinating these security responsibilities. Amazon Air has also assumed security responsibility for performing cargo acceptance and chain of custody; cargo screening, buildup, and consolidation; recordkeeping; cargo training; aircraft searches; screening jump seaters<sup>14</sup> and their property; incident reporting; comparing jump seaters and individuals who have access to aircraft and cargo against watchlists; and participation in table top exercises.

To address the current and anticipated demand, Amazon Air is increasing use of its own employees for company services and operations, rather than contracting out for services. Thus, Amazon Air will quickly hire new employees as it expands its operations at regulated airports. Hiring surges can occur at all airports throughout the year due to seasonal changes, construction, or other matters. Most airports can plan ahead for these surges to ensure sufficient staffing in the airport badging offices to begin the vetting process and issue ID media to new employees. However, when a new or existing employer has a significant, sudden increase in employees, all airport vendors can be adversely affected by the

strain this places on the airport badging system. It takes significant time to collect the biometric and biographic information needed to initiate CHRCs and security threat assessments (STAs), adjudicate CHRCs, and issue the ID media.

Amazon Air has represented to TSA that it has the capability and capacity to assume security responsibilities at other locations in addition to CVG, BWI, and RFI, including ensuring physical control of access points; adjudicating CHRCs for disqualifying offenses and submitting STAs for its employees; issuing ID media; and conducting ID media accountability audits. Amazon Air possesses sophisticated access control and monitoring systems that enhance security by significantly restricting access to cargo and aircraft. As a subsidiary of a profitable, private sector leader in technology, Amazon Air benefits from ample resources to purchase advanced equipment as needed, without regard to local government budget restrictions that many airports face. This factor provides a level of assurance that the security capability will remain consistent and substantial. Amazon Air's independent economic stability also provides a level of assurance that it will be able to quickly obtain any necessary expertise to carry out all of the EAA functions at additional locations going forward.

#### Authority and Determination

TSA may grant an exemption from a regulation if TSA determines that the exemption is in the public interest.<sup>15</sup> TSA finds this exemption to be in the public interest for several reasons. First, TSA has evaluated Amazon Air's security apparatus with respect to access control and monitoring, vetting and ID media issuance, and cargo management and movement, and determined it to be modern, strong, and resilient. Second, Amazon Air's significant personnel expansion at airports may strain the resources of airport operator and aircraft operator badging offices, adversely affecting other airport vendors and limiting new hire capability. Amazon Air's ability under an EAA to initiate the employee vetting functions that the airport authorities would otherwise be required to conduct will more efficiently manage volume as needed. This factor should reap economic benefits for the surrounding areas in terms of employment, and to other airport vendors who will not experience adverse effects from a sudden increase in airport ID media issuance. Moreover,

extending the authorities under an EAA to Amazon Air at additional airport locations is consistent with Executive Order 13725<sup>16</sup> to promote competition and reduce regulatory restrictions where possible. Finally, under an EAA, TSA will have direct oversight of Amazon Air's security activities, rather than indirectly through an aircraft operator, for which Amazon Air is an authorized representative. Given the scale of Amazon Air's commercial activities and physical infrastructure that must be secured at these airports, TSA compliance oversight will be more efficient and effective if conducted directly over Amazon Air.

Therefore, TSA has determined that it is in the public interest to grant eligible airport operators an exemption from the provision in 49 CFR 1542.111 that limits the persons with whom an airport operator may execute an EAA to aircraft operators and foreign air carriers. Under this Exemption and in accordance with the requirements set forth below, eligible airport operators may enter into an EAA with Amazon Air.

First, Amazon Air will assume responsibility for the vetting and identification media requirements that apply to individuals with unescorted access to the SIDA. These requirements include collecting and transmitting biographic and biometric information needed to conduct CHRCs, a check of government watchlists, and an immigration check. Also, Amazon Air will issue airport-approved ID media to the individuals who successfully complete the vetting process.

Second, at least 45 days prior to submitting the EAA/ASP amendment to the TSA Federal Security Director (FSD) at the airport for approval, the airport operator must notify the FSD and TSA's Assistant Administrator of Policy, Plans, and Engagement in writing, stating its interest in executing an EAA and requesting any documentation the parties must have to move forward with the EAA. Note that this 45-day notice provision is currently required when an airport operator seeks to amend its ASP. This 45-day notice will provide TSA sufficient time to evaluate the necessity and advisability of the EAA at that location.

Third, the airport operator and Amazon Air must first obtain all information from TSA that is necessary to execute the EAA prior to executing it. For instance, the parties must have the most recent EAA template issued by

<sup>12</sup> See 49 CFR 1544.101(h) for scope of a full all-cargo security program.

<sup>13</sup> These full all-cargo aircraft operators include Atlas Air, Air Transport International, ABX, Inc., and Sun Country Airlines.

<sup>14</sup> The term 'jump seater' refers to an off duty commercial pilot who is permitted to travel by using the jumpseat in the cockpit of a commercial aircraft operator.

<sup>15</sup> See 49 U.S.C. 114(q).

<sup>16</sup> *Steps to Increase Competition and Better Inform Consumers and Workers to Support Continued Growth of the American Economy*, April 15, 2016.

TSA, an approved Alternative Measure on file regarding Amazon-issued ID media, and a temporary technical policy regarding STA submissions.

### Exemption

1. This Exemption applies to airport operators regulated under 49 CFR 1542.103(a)–(b).
2. The Exemption takes effect on January 17, 2023.
3. For the duration of this Exemption, the eligible airport operators may apply for an amendment to their airport security program that permits the airport operator to enter into an EAA in accordance with 49 CFR 1542.111 with Amazon Air, notwithstanding that Amazon Air is not a TSA-regulated aircraft operator or foreign air carrier.
4. The airport operator must provide written notice of its intent to seek an EAA and ASP Amendment to the FSD and TSA's Assistant Administrator for Policy, Plans, and Engagement at least 45 days prior to submitting the EAA and ASP amendment.
5. The airport operator may not execute the EAA with Amazon Air until the airport operator and Amazon Air have received all information from TSA that is necessary to execute the EAA. Each airport operator seeking the EAA must receive an Alternative Measure that permits the airport operator to designate Amazon ID media as airport-approved. TSA may also require additional documentation to be on file as circumstances warrant.
6. The terms of the EAA replace requirements set forth in 49 CFR part 1542 so long as Amazon Air complies with the EAA.
7. The EAA must require Amazon Air to comply with all relevant Security Directives and Emergency Amendments issued by TSA.
8. Amazon Air may begin performing as an EAA-holder on the date on which TSA approves an amendment to the respective airport operator's airport security program implementing each executed EAA.
9. The Exemption will remain in effect while the airport operator's TSA-approved airport security program remains in effect. TSA may direct revisions to the ASP amendment and EAA for security reasons in accordance with 49 CFR 1542.105(c). TSA may rescind the ASP amendment and EAA, and may rescind or modify the Exemption, with regard to one or more of the covered airport operators, at any time.

Dated: January 10, 2023.

**David P. Pekoske,**

*Administrator.*

[FR Doc. 2023–00647 Filed 1–13–23; 8:45 am]

**BILLING CODE 9110–05–P**

## DEPARTMENT OF THE INTERIOR

### Geological Survey

**[GX.23.ZQ00.F0804.00; OMB Control Number 1028–NEW]**

#### Agency Information Collection Activities: User Testing of Graphics for USGS Aftershock Forecasts

**AGENCY:** U.S. Geological Survey (USGS), Interior.

**ACTION:** Notice of information collection; request for comment.

**SUMMARY:** In accordance with the Paperwork Reduction Act of 1995 (PRA), the U.S. Geological Survey (USGS) is proposing to begin a new information collection.

**DATES:** Interested persons are invited to submit comments on or before March 20, 2023.

**ADDRESSES:** Send your comments on this information collection request (ICR) by mail to U.S. Geological Survey, Information Collections Officer, 12201 Sunrise Valley Drive MS 159, Reston, VA 20192; or by email to [gs-info\\_collections@usgs.gov](mailto:gs-info_collections@usgs.gov). Please reference OMB Control Number 1028–NEW in the subject line of your comments.

**FOR FURTHER INFORMATION CONTACT:** To request additional information about this ICR, contact Sara McBride by email at [skmcbride@usgs.gov](mailto:skmcbride@usgs.gov) or by telephone at 650–750–5270. Individuals in the United States who are deaf, deafblind, hard of hearing, or have a speech disability may dial 711 (TTY, TDD, or TeleBraille) to access telecommunications relay services. Individuals outside the United States should use the relay services offered within their country to make international calls to the point-of-contact in the United States.

**SUPPLEMENTARY INFORMATION:** In accordance with the PRA (44 U.S.C. 3501 *et seq.*) and 5 CFR 1320.8(d)(1), all information collections require approval. We may not conduct or sponsor, nor are you required to respond to, a collection of information unless it displays a currently valid OMB control number.

As part of our continuing effort to reduce paperwork and respondent burdens, we invite the public and other Federal agencies to comment on new, proposed, revised, and continuing

collections of information. This helps us assess the impact of our information collection requirements and minimize the public's reporting burden. It also helps the public understand our information collection requirements and provide the requested data in the desired format.

We are especially interested in public comment addressing the following:

- (1) Whether or not the collection of information is necessary for the proper performance of the functions of the agency, including whether or not the information will have practical utility;
- (2) The accuracy of our estimate of the burden for this collection of information, including the validity of the methodology and assumptions used;
- (3) Ways to enhance the quality, utility, and clarity of the information to be collected; and
- (4) How the agency might minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, *e.g.*, permitting electronic submission of response.

Comments that you submit in response to this notice are a matter of public record. We will include or summarize each comment in our request to OMB to approve this ICR. Before including your address, phone number, email address, or other personally identifiable information (PII) in your comment, you should be aware that your entire comment—including your PII—may be made publicly available at any time. While you can ask us in your comment to withhold your PII from public review, we cannot guarantee that we will be able to do so.

**Abstract:** The USGS produces and releases forecasts for earthquake aftershocks following damaging earthquakes in an automated manner. Currently, these forecasts are communicated to the public and to specialist users in text and tabular formats. The aim of this project is to produce graphics and maps for aftershock forecasts that can better serve user needs. To ensure new forecast graphics serve user needs, we will conduct online user testing. In this information collection, we will anonymously ask users questions about a variety of graphical representations of the forecast. This will help identify how different graphics affect users' understanding and use of aftershock forecast information. The results of this user testing will improve the way the USGS communicates aftershock forecasts to the public.